5. (Amended) Computing apparatus according to claim 3, wherein the trusted device is arranged to transfer the instructions to the main processing means in response to memory read signals from the main processing means.

6. (Amended) Computing apparatus according to claim 1, wherein the trusted device comprises device memory means and is arranged to monitor a data bus means by which components mounted on the assembly are adapted to communicate and store in the device memory means a flag in the event the first memory read signals generated by the main processing means after the computing apparatus is released from reset are addressed to the trusted device.

92

7. (Amended) Computing apparatus according to claim 1, wherein the trusted device has stored in device memory means at least one of:

a unique identity of the trusted device;

an authenticated integrity metric generated by a trusted party; and

a secret.

10. (Amended) Computing apparatus according to claim 8, wherein the trusted device has stored in device memory means an authenticated integrity metric generated by a trusted party and includes a encryption function, the trusted device being arranged to generate a response to a received challenge, the response comprising an acquired integrity metric and the authenticated integrity metric, both signed by the encryption function using the private asymmetric encryption key.

93

Please cancel claim 11 without prejudice.

12. (Amended) A method of operating a system comprising a trusted computing apparatus and a user, the trusted computing apparatus incorporating a trusted device being arranged to acquire the true value of an integrity metric of the trusted computing apparatus, the method comprising the steps of:

the trusted device acquiring the true value of the integrity metric of the trusted computing apparatus;

the user generating a challenge for the trusted computing apparatus to prove its integrity and submitting the challenge to the trusted computing apparatus;

the trusted computing apparatus receiving the challenge, and the trusted device generating a response including the integrity metric and returning the response to the user; and

the user receiving the response, extracting the integrity metric from the response and comparing the integrity metric with an authenticated metric for the trusted computing apparatus that had been generated by a trusted party.

16. (Amended) A method of establishing a communications channel in a system between trusted computing apparatus and remote computing apparatus, the method including the step of the remote computing apparatus verifying the integrity of the trusted computing apparatus using the method according to claim 12, and maintaining the communications channel for further transactions in the event the integrity of the trusted computing apparatus is successfully verified by the remote computing apparatus.

17. (Amended) A method of verifying that trusted computing apparatus is trustworthy for use by a user for processing a particular application, the method including the step of the user verifying the integrity of the trusted computing apparatus

using the method according to claim 12, and the user using the trusted computing apparatus to process the particular application in the event the integrity of the trusted computing apparatus is successfully verified by the remote computing apparatus.

Please cancel claims 18-21 without prejudice.

Please add the following new claims:

22. (New) Computing apparatus comprising an assembly; a main processor, a main memory and a trusted device, each being mounted on the assembly and connected for communication with other components mounted on the assembly, wherein the trusted device is adapted to acquire a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric.

23. (New) Computing apparatus as claimed in claim 22, wherein the integrity metric is a digest of all or part of the basic input/output software for the computing apparatus.

24. (New) Computing apparatus as claimed in claim 22, wherein the integrity metric is a digest of all or part of the basic input/output software for components or apparatus attached to the computing apparatus.

25. (New) Computing apparatus as claimed in claim 22, wherein the trusted device is adapted to acquire a plurality of integrity metrics.

26. (New) Computing apparatus as claimed in claim 22, wherein

the trusted device is adapted to be tamper resistant.

27. (New) Computing apparatus as claimed in claim 22, wherein the trusted device comprises a device memory.

28. (New) Computing apparatus as claimed in claim 27, wherein the trusted device comprises a trusted device processor.

29. (New) Computing device as claimed in claim 28, wherein the trusted device processor is adapted to instruct the main processor to determine the integrity metric and return the integrity metric for storage in the device memory.

30. (New) Computing apparatus as claimed in claim 28, wherein the trusted device processor is adapted to obtain information necessary to calculate the integrity metric and to calculate the integrity metric for storage in the device memory.

31. (New) Computing apparatus as claimed in claim 28, wherein the trusted device has a secret stored in the device memory.

32. (New) Computing apparatus as claimed in claim 31, wherein the secret comprises a private asymmetric encryption key.

33. (New) Computing apparatus as claimed in claim 32, wherein the trusted device also has stored in the device memory in the device memory a respective public encryption key that has been signed by a trusted third party.

34. (New) Computing apparatus as claimed in claim 33, wherein the trusted device also has stored in the device memory an authenticated integrity metric generated by a trusted third party and wherein the trusted device is adapted to employ an

encryption function, the trusted device processor being arranged to generate a response to a received challenge, the response comprising an acquired integrity metric and the authenticated integrity metric, both signed by the encryption function using the private asymmetric encryption key.

35. (New) In a computing apparatus comprising an assembly, a plurality of functional components including a main memory and a main processor mounted on the assembly, each functional component being connected for communication with one or more other functional components on the assembly, a trusted device being one of said functional components and adapted to acquire a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric.

36. (New) A trusted device for use as a functional component in a computing apparatus, the trusted device being adapted for mounting on an assembly of the computing apparatus and being adapted for communication with other functional components of the computing apparatus, the trusted device being adapted to acquire a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric.

37. (New) Computing apparatus as claimed in claim 36, wherein the trusted device is adapted to be tamper resistant.

38. (New) Computing apparatus as claimed in claim 36, wherein the trusted device comprises a device memory.

39. (New) Computing apparatus as claimed in claim 38, wherein the trusted device comprises a trusted device processor.

40. (New) Computing apparatus as claimed in claim 39, wherein the trusted device has a secret stored in the device memory.

41. (New) Computing apparatus as claimed in claim 40, wherein the secret comprises a private asymmetric encryption key.

42. (New) Computing apparatus as claimed in claim 41, wherein the trusted device also has stored in the device memory in the device memory a respective public encryption key that has been signed by a trusted third party.

43. (New) Computing apparatus as claimed in claim 42, wherein the trusted device also has stored in the device memory an authenticated integrity metric generated by a trusted third party and wherein the trusted device is adapted to employ an encryption function, the trusted device processor being arranged to generate a response to a received challenge, the response comprising an acquired integrity metric and the authenticated integrity metric, both signed by the encryption function using the private asymmetric encryption key.

REMARKS

This Preliminary Amendment clarifies some of the terms in the claims. Such amendments to claims 1 and 2 do not affect the scope of those claims. New claims 22-43 have been added after International Preliminary Examination.

This Preliminary Amendment also amends Claims 5-7, 10 and 16-17 so that these claims are no longer multiply dependent to reduce